



Section II: Administrative Security
Title: Information Classification Security Standard
Current Effective Date: June 30, 2008
Revision History: June 11, 2008
Original Effective Date: June 30, 2008

Purpose: To ensure that all North Carolina (NC) Department of Health and Human Services (DHHS) data and/or information are properly classified, labeled, and managed.

STANDARD

1.0 Background

The Divisions and Offices management must ensure that data is properly labeled, stored, and handled to ensure data confidentiality, integrity, and availability. In addition, the Divisions and Offices must establish their own policies, procedures, standards, and guidelines, as defined in this standard.

2.0 Classifying DHHS Information

All Divisions and Offices shall effectively classify data and/or information as *confidential* or *public*. Confidentiality is to be determined in accordance with NC General Statutes (N.C.G.S.) – Chapter 132 Public Records and all other applicable legal and regulatory requirements. The DHHS data and/or information must be given the same classification regardless of the storage media method (e.g., tapes, disks, CDs, cassettes, USB flash memory drives, etc.). In addition, all Divisions and Offices shall maintain a comprehensive and up-to-date data and/or information inventory. The Divisions and Offices information inventory must be periodically reviewed to ensure confidentiality, integrity, and availability.

Only the DHHS system owner or the designee can authorize reclassification of data and/or information. When data and/or information are reclassified, the DHHS system owner's supervisor must notify the data stewards immediately.

3.0 Storing and Handling Classified Information

All data and/or information shall be handled in a manner that effectively secures and safeguards the confidentiality, integrity, and availability of DHHS data and/or information, against any type of inherent risk. For information related to the storage and handling of classified data and/or information, please refer to the NC DHHS Security Standards, Administrative Security Standards – Data Stewardship Security Standard.

4.0 DHHS Federal Information





When Divisions and Offices receive classified information from the United States (US) Federal Government, such information shall be stored in a separate secure location. The US Federal Government information must be properly handled in accordance with Title 13 – Protection of Confidential Information, Section 9: Information as Confidential Exception and Section 214: Wrongful Disclosure of Information.

5.0 Ownership of DHHS Data

The DHHS data stewards or designees shall be responsible for securing data by establishing procedures that govern how data is handled in Divisions and Offices.

6.0 Employment and Confidential Information

When a workforce member is terminated, promoted, or transferred, the workforce member's supervisor shall be responsible for transferring custody of confidential data and/or information. The workforce member's supervisor shall ensure that data and/or information custody is relayed immediately to the DHHS system owner or a designee.

7.0 Information Utilized by DHHS Third-Party Contractors

All the data and/or information utilized by third-party contractors shall be routinely reviewed and monitored by appropriate Division and Office management.

Reference

- US Federal Government
 - Title 13 – Protection of Confidential Information
 - Section 9: Information as Confidential Exception
 - Section 214: Wrongful Disclosure of Information
- HIPAA Administration Simplification Act - 45 C.F.R. Parts 160 and 164.
 - HIPAA – 45 C.F.R. § 164.308(a)(3) Workforce Security.
 - HIPAA – 45 C.F.R. § 164.308(a)(7) Contingency Plan.
 - HIPAA – 45 C.F.R. § 164.308(a)(7)(ii)(A) Data Backup Plan.
 - HIPAA – 45 C.F.R. § 164.308(a)(8) Evaluation.
 - HIPAA – 45 C.F.R. § 164.310(a)(1) Facility Access Controls.
 - HIPAA – 45 C.F.R. § 164.310(d)(1) Device and Media Controls.
 - HIPAA – 45 C.F.R. § 164.312(e)(1) Transmission Security.
- North Carolina General Statutes
 - N.C.G.S. Chapter 132. Public Records.
- NC Statewide Information Security Manual, Version No.1
 - Chapter 1 – Classifying Information and Data, Section 01: Setting Classification Standards
 - Standard 010101 – Defining Information
 - Standard 010102 – Labeling Classified Information





-
- Standard 010103 – Storing and Handling Classified Information
 - Standard 010104 – Isolating Top Secret Information
 - Standard 010105 – Classifying Information
 - Standard 010106 – Accepting Ownership for Classified Information
-
- NC DHHS Security Standards Manual
 - Administrative Security Standards
 - Data Stewardship Security Standard
 - NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
 - Data Classification, Labeling, and Access Control Policy

